Розвиток силової витривалості засобами гирьового спорту позитивно впливає на фізичну підготовленість курсантів про що, свідчить проведене дослідження.

Перспективним напрямком подальших досліджень є поглиблене вивчення засобів гирьового спорту з метою вдосконалення психофізичної підготовленості майбутніх офіцерів Національної поліції України.

Список бібліографічних посилань

1. Архангородський З. С. Гирьовий спорт. Київ : Здоров'я, 1980. 72 с.
2. Грибан Г. П., Ткаченко П. П. Основи підготовки у гирьовому спорті : навч.-метод. посіб. Житомир : Рута, 2013. 102 с.
3. Рассказов В. С. Пути и перспективы развития гиревого спорта. М. : МФГС, 2004. 33 с.
4. Фізичне виховання : навч. посіб. / С. І. Присяжнюк, В. П. Краснов, М. О. Третьяков та ін. Київ : Центр учб. літ., 2007. 192 с.
5. Физическая подготовка военнослужащих к действиям в особых условиях : учеб. пособие / под ред. М. Лаговского. СПб. : Питер, 1996. 135 с.

Надійшла до редколегії 03.04.2019

УДК 65.012.8+004

О. В. МАНЖАЙ,
кандидат юридичних наук, доцент,
доцент кафедри кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ;
https://orcid.org/0000-0001-5435-5921

ОСОБЛИВОСТІ АНАЛІТИЧНОЇ І ТЕХНІЧНОЇ СКЛАДОВОЇ ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Розглядаються окремі питання аналітичної та технічної складової підготовки фахівців для Національної поліції України. Аналізуються проблемні питання в цій сфері. Пропонуються конкретні шляхи підвищення кваліфікації працівників Національної поліції з урахуванням можливостей сучасних комп'ютерних технологій. Розглядаються декілька шляхів підготовки фахівців у сфері протидії кіберзлочинності.

Ключові слова: *підготовка фахівців, аналітична складова, технічна складова, поліція.*

Аналіз сучасних тенденцій в роботі правоохоронних органів розвинених країн світу засвідчує зростання рівня застосування комп'ютерних технологій та аналітичного апарату для протидії злочинності та забезпечення публічної безпеки і порядку. В країнах Європейського союзу та США ще з середини 90-х років XX століття почали інтенсивно впроваджувати нові моделі в діяльності поліції. Найбільш поширеною серед них сьогодні є модель на основі розвідувальних даних (intelligence-led policing), проте і вона в перспективі вже має заміну. Прогностична модель (predictive policing) як найбільш інноваційна вже сьогодні впроваджується в якості пілотного проекту у найбільш технічно оснащених відділах поліції, здебільшого в рамках заходів з випробовування технологічними компаніями нових рішень у сфері штучного інтелекту та обробки великих даних (big data). У загальному випадку її мету можна позначити як передбачення місця, суб'єкта, часу, особи жертви вчинення конкретного злочину.

Українські поліцейські поки що значно відстають від зарубіжних колег у в провадженні новітніх технологій розслідування. Це пов'язано з багатьма факторами, головним з яких, звичайно, є хронічна нестача фінансового та матеріального забезпечення. Непоодинокими випадками є відсутність належної кількості якісної комп'ютерної техніки в необхідній

кількості навіть у підрозділах кіберполіції, не говорячи вже про ситуацію в невеликих населених пунктах. В цілому реформування сучасної поліцейської діяльності в Україні стикається з багатьма труднощами, що обумовлені як суб'єктивними, так і об'єктивними факторами.

Вказане обумовлює незначні стартові можливості для покращення ситуації, проте, навіть в умовах обмежених ресурсів, можна здійснити кроки, які підвищать ефективність практичної складової за рахунок впровадження інноваційних рішень.

Для прикладу візьмемо типовий оперативний підрозділ в міському відділі поліції, який має такі вхідні характеристики:

– один комп'ютер на 3–5 працівників;

– відсутність доступу до державних реєстрів, крім Інтегрованої інформаційно-пошукової системи («АРМОР») на обмеженій кількості робочих місць;

– недостатня кваліфікація оперативних працівників по роботі з комп'ютерною технікою.

Працівники цього підрозділу з кожним роком все більше стикаються з ситуаціями, коли:

– доказова інформація або засоби доступу до такої інформації зберігаються за допомогою комп'ютерної техніки (ПК, серверів, смартфонів тощо). Причому використовуються різні операційні системи, що ще більше ускладнює ситуацію;

– черга на проведення комп'ютерно-технічної експертизи знижує ефективність розслідування;

– конкуренція, а також дотримання вимог конспірації роблять не завжди можливою взаємодію між підрозділами в сфері проведення аналітичної обробки накопичених даних та проведення дій і заходів з добування інформації, пов'язаних із застосуванням комп'ютерних технологій.

Вирішення окремих з позначених проблемних питань можливе шляхом підвищення кваліфікації оперативних працівників, загальний девіз якого має бути: «Прості речі з електронними даними можна робити самим». Проведення відповідних занять слід організувати з використанням доступного програмного забезпечення з вільною ліцензією.

У рамках проведення означеного підвищення кваліфікації пропонується приділити увагу:

– роз'ясненню механізмів та шляхів *отримання доступу до різних інформаційних ресурсів*, у тому числі державних реєстрів, зокрема Державного реєстру речових прав та підсистеми НАІС Єдиного державного реєстру МВС;

– навчанню різним способам та інструментам *пошуку інформації* в комп'ютерних мережах за різними ідентифікаторами;

– використанню *систем кримінального аналізу* для протидії злочинності та забезпечення публічної безпеки і порядку;

– *правильному складанню запитів* про отримання інформації від технологічних компаній;

– розкриттю методів і засобів *пришвидшення аналізу документів*, що надходять від банківських установ, мобільних операторів, провайдерів тощо та містять великий об'єм даних;

– *систематизації великих об'ємів даних*;

– *візуалізації зв'язків* за результатами аналізу великих об'ємів даних;

– навчанню простим засобам і методам швидкого автоматизованого вилучення даних та *огляду електронних доказів*;

– *використання електронного підпису* при роботі з електронним доказами;

– *поєднанню та автоматизації технік DFINT* (digital forensic intelligence) *OSINT* (open source intelligence) для досягнення цілей оперативно-розшукової діяльності та досудового слідства;

– використання *систем розпізнавання облич* для вирішення завдань оперативно-службової діяльності.

Стосовно останнього пункту хотілося б відмітити, що в Національній поліції чомусь досі не розроблено систему розпізнавання обличчя особи за фотографією, де у якості бази для порівняння могли б виступати зображення, які містяться в Інтегрованій інформаційно-пошуковій системі. Існують запрограмовані алгоритми такого розпізнавання на основі

штучного інтелекту з вільною ліцензією, які б могли бути використані в роботі правоохоронних органів без необхідності виділення додаткових фінансових ресурсів, крім, звичайно, інфраструктурних витрат та витрат на серверне обладнання.

У якості прикладів відповідних інструментів, для розв'язання окремих задач, можна навести нейромережу DarkNet [1] та модель Yolo [2]; проект Face Recognition [3]. Опис самої процедури розпізнавання можна знайти, наприклад, за адресою: https://sohabr.net/habr/post/306568/ [4]. Описану систему вже запущено в багатьох приватних проектах, у тому числі громадських, як от identigraf.center.

В масштабах такого органу як Національна поліція створення описаної системи є не надто складним завданням. Водночас забезпечення доступу до неї територіальних підрозділів могло б в рази підвищити їх ефективність в частині протидії злочинності, розшуку безвісти зниклих осіб, розпізнавання осіб невпізнаних трупів.

Що стосується підготовки фахівців вузького профілю, як от для підрозділів кіберполіції, то відповідні пропозиції було викладено нами раніше в [5]. Зміст та інтенсивність відповідного навчання залежатиме від обраного плану такої підготовки. Вказані плани умовно можна поділити на оперативний, тактичний та стратегічний.

Оперативний план передбачає інтегровану ступеневу модель підготовки фахівців. На першому етапі (цей етап вже впроваджується в Україні) здійснюється набір до патрульної поліції. Після визначеного строку роботи в патрульній поліції (наприклад, 1 рік) патрульні, які мають вищу освіту, одержують право пройти додаткові курси (6 місяців) зі спеціалізації «протидія кіберзлочинності» за умови попереднього конкурсного відбору. Фахівці, які успішно склали іспити за підсумками курсів, мають право зайняти первинні посади у підрозділах кіберполіції. У наступному кожні 3 роки означені фахівці мають проходити 3-місячні курси підвищення кваліфікації у відповідних установах. Підготовку має здійснювати один з вищих навчальних закладів МВС України.

Переваги:

– ступенева підготовка дозволяє відібрати найбільш мотивованих фахівців, які мають досвід роботи на первинних посадах поліції;

– скорочений термін підготовки фахівців дозволяє зекономити кошти.

Недоліки:

– швидкий розвиток комп'ютерних технологій передбачає постійну самоосвіту відповідних фахівців. Випадання патрульних з цього процесу на час служби в патрульній поліції не дозволяє говорити про підготовку високоякісних фахівців у сфері високих технологій (у переважній більшості), які зможуть ефективно протидіяти дійсно кваліфікованому кіберзлочинцю;

– не можна впевнено говорити про підготовку ефективного фахівця, якщо він не має знань рівня «кваліфікований користувач» або «професіонал» у сфері комп'ютерної техніки.

Тактичний план передбачає підготовку фахівців у сфері протидії кіберзлочинності через додаткову профільну адоптацію їх знань для роботи в правоохоронних органах. Вказаний план реалізується за допомогою початкової підготовки фахівців з технічною або юридичною освітою, яку вони здобули у цивільних вишах. Курс навчання – 6 місяців. Конкретні дисципліни залежатимуть від одержаних в університеті знань фахівця (юридичні або технічні науки).

Переваги:

– змога одержати кваліфікованого фахівця без додаткових затрат бюджетних коштів (проте ця перевага нівелюється, якщо студент вчився за державним замовленням);

– скорочений термін підготовки фахівців дозволяє оперативніше змінювати зміст бази знань, яку вони мають набути.

Недоліки:

– підготовка означених фахівців у цивільних вишах викликає низку складнощів, основною з яких є те, що значна частина відповідних нормативних документів та методик протидії кіберзлочинності мають гриф обмеження доступу;

– заробітна платня фахівця відповідної кваліфікації у приватному секторі економіки у декілька разів перевищує аналогічний показник у МВС України, що робить нераціональною підготовку відповідних фахівців.

Стратегічний план передбачає підготовку фахівців на базі вищих навчальних закладів системи МВС України. Термін навчання – 3–4 роки. Таку підготовку доцільно здійснювати на базі технічного напряму підготовки із можливістю на контрактній основі паралельного одержання вищої юридичної освіти. Вказане обумовлене тим, що технічному фахівцю і системним мисленням здебільшого набагато простіше набути юридичні знання, аніж технічно непідготовленому фахівцю у сфері права.

Переваги:

– органічне поєднання технічних та юридичних знань, що є важливим для працівника підрозділів кіберполіції;

– систему підготовки можна здійснити на створеній базі вишів системи МВС України, курсант по закінченні вищого навчального закладу МВС України має дотримуватися умов контракту, що стримує його звільнення з Національної поліції України.

Недоліки:

– тривалий час підготовки фахівця;

– затрати на утримання вишів (нівелюється, якщо зважати на те, що держава все одно набирає на навчання громадян за державним замовленням).

Підсумовуючи, зазначимо, що питанню технічної та аналітичної підготовки фахівців для підрозділів Національної поліції потрібно вже сьогодні приділити прискіпливу увагу. Вказане обумовлено часом, рівнем техніки та необхідністю збереження переваги над злочинністю. Невипадково у США за штатним розкладом на одного польового агента ФБР вже сьогодні припадає декілька технічних фахівців та аналітиків. Україна на теперішній час не може дозволити собі таких витрат, тому найбільш раціональним буде набуття всіма поліцейськими, принаймні, базових технічних та аналітичних знань.

Список бібліографічних посилань

1. Darknet: Open Source Neural Networks in C. URL: https://pjreddie.com/darknet/ (дата звернення: 28.04.2019).

2. YOLO: Real-Time Object Detection. URL: https://pjreddie.com/darknet/yolo/ (дата звернення: 28.04.2019).

3. Ageitgey/face_recognition URL: https://github.com/ageitgey/face_recognition (дата звернення: 28.04.2019).

4. Лукин Б. Обучение машины – забавная штука: современное распознавание лиц с глубинным обучением // habr : сайт. URL: https://sohabr.net/habr/post/306568/ (дата звернення: 28.04.2019).

5. Манжай О. В., Галауз В. Є. Шляхи підготовки фахівців у сфері протидії кіберзлочинності // Актуальні питання протидії кіберзлочинності та торгівлі людьми : зб. матеріалів Всеукр. наук.-практ. конф. (м. Харків, 23 листоп. 2018 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. Харків : Харків. нац. ун-т внутр. справ, 2018. С. 350–352.

Надійшла до редколегії 29.04.2019